

Forum:[Hack Forums](#)

Thread: [Do people modify public Bots/do it all the time and release them in the wild?](#)

ExecutionTricks - January 26, 2019, 12:21 pm

I've heard of Owari, Muhstik, and other variants of Mirai, are there dozens if not hundreds or thousands of other variants not even reported out there right now and more being made as we speak?

also is it common practice to take code like one feature from one public Botnet and put it in yours/Frankenstien together features like this?

Ramb0x - January 26, 2019, 12:25 pm

Does anybody have have muhstik source code or some material about SOCKS4 protocol how does they connect to internet.

If so please post here or pm me.

ExecutionTricks - January 26, 2019, 12:31 pm

(Jan 26, 2019 01:25 PM)spix Wrote: [\[CITE\]](#) Does anybody have have muhstik source code or some material about SOCKS4 protocol how does they connect to internet.

If so please post here or pm me.

I cannot help but I wish you luck :)

I don't know if Muhstik's source has been released on the internet it was just an article covering it and mettle and hajime, and satori. I know satori had a second Botnet that was even better I believe. Everyone should try to get Satori's works if you're trying for anything Mirai.

blog.netlab.360 . com/gpon-exploit-in-the-wild-i-muhstik-botnet-among-others-en/

mettle: the attacker utilizes the IP address in Viet Nam (C2 210.245.26.180:4441,scanner 118.70.80.143) and open-sourced Mettle attack module to implant of malware. It is the first time we observe this botnet.

muhstik: We first disclose this botnet last month (report-2018-04). In the latest update, Muhstik added exploits for the three vulnerabilities: GPON (cve-2018-10561, cve-2018-10562), JBOSS (cve-2007-1036) and DD-WRT (Web Authentication Bruteforcing).

Mirai (more than one variants): After opensourced on 2016-09, mirai botnet has been used by hundreds of malicious gangs. This time we observe that more than one groups are actively using this exploit to deliver their mirai variants

hajime:We have released two reports on Hajime botnets(Report-2017-09 , Briefing-2018-03). Hajime also did the update this time and began to infect GPON related devices.

satori:satori botnet was first disclosed by us as well, which infected 260,000 devices in 12 hours in 2017-12 (report-2017-11, report-2017-12, report-2018-01). We observed that Satori also added

GPON vulnerability exploit in the latest update.

I.M.P - January 26, 2019, 12:32 pm

Actually to answer your question, no people don't just Frankenstein bots together, because of the payload. You can't just take any old feature from one bot and slam it into another

ExecutionTricks - January 26, 2019, 12:33 pm

(Jan 26, 2019 01:32 PM)Atroxcity Wrote: [\[CITE\]](#) Actually to answer your question, no people don't just Frankenstein bots together, because of the payload. You can't just take any old feature from one bot and slam it into another

Even if you have the source code of course, and the type of Botnet has a similar infrastructure, protocols, and languages? I guess then maybe it could work depending on the feature?

I.M.P - January 26, 2019, 12:35 pm

(Jan 26, 2019 01:33 PM)ExecutionTricks Wrote: [\[CITE\]](#) Even if you have the source code of course, and the type of Botnet has a similar infrastructure, protocols, and languages? I guess then maybe it could work depending on the feature?

Once again, it's impossible because the panel sends a command to the payload, and that command has an internal name, it's complicated to explain

ExecutionTricks - January 26, 2019, 12:37 pm

(Jan 26, 2019 01:35 PM)Atroxcity Wrote: [\[CITE\]](#) Once again, it's impossible because the panel sends a command to the payload, and that command has an internal name, it's complicated to explain
OK fair, if you can't explain/it's difficult no worries.

But I read about Muhstick.

And is it like from here the muhstik.scanner, muhstik.infector, etc, is there no way to modify these/internal name? Do I not build the panel and payload? So when building I could do that, or modify the builder?

Scanning phase:muhstik.scanner will initiate scanning and exploit the vulnerability to force vulnerable GPON devices to report status to the reporting server;

Infection phase:muhstik.infector will exploit vulnerability to force GPON susceptible devices to download malware from the download server and install it.

Control phase:muhstik.c2.list will send commands to its bots and request them to launch scanning, SSH scale-out, xmrig Mining, cgminer mining, or DDoS attacks.

(Jan 26, 2019 01:35 PM)Atroxcity Wrote: [\[CITE\]](#) Once again, it's impossible because the panel sends a command to the payload, and that command has an internal name, it's complicated to explain

Can you use if source code is available parts of different variants of Mirai specifically with each other/with the base Mirai at least?

I.M.P - January 26, 2019, 1:01 pm

(Jan 26, 2019 01:37 PM)ExecutionTricks Wrote: [\[CITE\]](#) OK fair, if you can't explain/it's difficult no worries.

But I read about Muhstick.

And is it like from here the muhstik.scanner, muhstik.infector, etc, is there no way to modify these/internal name? Do I not build the panel and payload? So when building I could do that, or modify the builder?

Scanning phase:muhstik.scanner will initiate scanning and exploit the vulnerability to force vulnerable GPON devices to report status to the reporting server;

Infection phase:muhstik.infector will exploit vulnerability to force GPON susceptible devices to download malware from the download server and install it.

Control phase:muhstik.c2.list will send commands to its bots and request them to launch scanning, SSH scale-out, xmrig Mining, cgminer mining, or DDoS attacks.

Can you use if source code is available parts of different variants of Mirai specifically with each other/with the base Mirai at least?
The payload.

Twistd - January 26, 2019, 2:35 pm

(Jan 26, 2019 01:35 PM)Atroxcity Wrote: [\[CITE\]](#) Once again, it's impossible because the panel sends a command to the payload, and that command has an internal name, it's complicated to explain Eh? If you have the source of course you can combine old features with new as you'd like, wtf are you even talking about? If you have the panel + payload source, what's stopping you from modifying it to whatever extent you want?

I.M.P - January 26, 2019, 2:40 pm

(Jan 26, 2019 03:35 PM)Twistd Wrote: [\[CITE\]](#) Eh? If you have the source of course you can combine old features with new as you'd like, wtf are you even talking about? If you have the panel + payload source, what's stopping you from modifying it to whatever extent you want?
Must be way different between rats and botnets ig

Twistd - January 26, 2019, 4:01 pm

(Jan 26, 2019 03:40 PM)Atroxcity Wrote: [\[CITE\]](#) Must be way different between rats and botnets ig
Why would it be different?

Alles auf Rot - January 26, 2019, 4:26 pm

(Jan 26, 2019 03:40 PM)Atroxcity Wrote: [\[CITE\]](#) Must be way different between rats and botnets ig
Its pretty simple to add more features as soon you have panel and payload src.. i dont see your problem there. Its easy in rats as in botnets..

I.M.P - January 26, 2019, 4:32 pm

(Jan 26, 2019 05:26 PM)Alles auf Rot Wrote: [\[CITE\]](#) Its pretty simple to add more features as soon you have panel and payload src.. i dont see your problem there. Its easy in rats as in botnets..
Nvm

Twistd - January 26, 2019, 5:03 pm

(Jan 26, 2019 05:32 PM)Atroxcity Wrote: [\[CITE\]](#) Nvm
?

ExecutionTricks - January 26, 2019, 6:14 pm

(Jan 26, 2019 06:03 PM)Twistd Wrote: [\[CITE\]](#) ?

(Jan 26, 2019 05:26 PM)Alles auf Rot Wrote: [\[CITE\]](#) Its pretty simple to add more features as soon you have panel and payload src.. i dont see your problem there. Its easy in rats as in botnets..
What I downloaded is apparently the Owari Botnet with Source Code. Unsure if SRC for Panel AND Payload or what.

So other Bots with the source code released I can take inspiration from and quality ones adopt and modify and improve? Or is there constrictions to the panel protocol or the languages things are coded in or does it kinda depend on that and more things that would depend on what Botnet source codes you were working with.

But Mirai Botnets with the SRC available should all pretty much work inherently with each other?

r4mbl3r - January 27, 2019, 11:26 pm

(Jan 26, 2019 07:14 PM)ExecutionTricks Wrote: [\[CITE\]](#)

What I downloaded is apparently the Owari Botnet with Source Code. Unsure if SRC for Panel AND Payload or what.

So other Bots with the source code released I can take inspiration from and quality ones adopt and modify and improve? Or is there constrictions to the panel protocol or the languages things are coded in or does it kinda depend on that and more things that would depend on what Botnet source codes you were working with.

But Mirai Botnets with the SRC available should all pretty much work inherently with each other?
I don't know anything about Mirai, but, in general, it should be possible to take inspiration from features in one program and implement them as modifications to a different program.

NoobySkid - January 29, 2019, 8:17 pm

It happens so often most public sources are shit tho

J?son - January 30, 2019, 7:29 pm

muhstik is not a form of mirai, you braindead retard

it's for loading proxies and flooding irc networks